UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/585,517 | 07/10/2006 | Saar Wilf | 2043.561US1 | 7666 |

49845 7590 03/14/2012
SCHWEGMAN, LUNDBERG & WOESSNER/EBAY
P.O. BOX 2938
MINNEAPOLIS, MN 55402

| EXAMINER | |
|---|---|
| MACILWINEN, JOHN MOORE JAIN | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2442 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 03/14/2012 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO@SLWIP.COM
SLW@blackhillsip.com

| | | | |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/585,517 | **Applicant(s)**<br>WILF ET AL. | |
| | **Examiner**<br>JOHN MACILWINEN | **Art Unit**<br>2442 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *12 December 2011*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

5)☒ Claim(s) *1-5,7,9-36,38,43,44 and 46-50* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)□ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-5,7,9-36,38,43,44 and 46-50* is/are rejected.

8)□ Claim(s) _____ is/are objected to.

9)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

10)□ The specification is objected to by the Examiner.

11)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *12/12/2011*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

## DETAILED ACTION

### *Response to Arguments*

***1.*** Applicant's arguments filed 12/12/2011 have been fully considered.

***2.*** On page 13, Applicant notes claim amendments and cancellations have been made, addressing the rejections made on pages 5 - 8 of the 8/10/2011 Non-Final Rejection in view of 35 U.S.C. 112, 2nd paragraph. Applicant's arguments are persuasive, and the grounds of rejection have thus been withdrawn.

***3.*** On pages 13 – 14, Applicant notes that claim 1 has been amended, incorporating language similar to language previously presented in dependent claims 20 and 21. Claims 20 and 21, depending on claim 1, previously recited:

> [claim 20] “wherein at least one of said feature of an original source of said first information element and of said potential relay device is a feature related to a configuration status"
>
> [claim 21] ... “wherein said feature related to a configuration status is selected from the group consisting of ... a software type” ...

Dependent claims 20 and 21 have both been presently amended.

Additionally, independent claim 1 has been amended to recite new, more precise claim language not previously presented. Claim 1 now recites:

> [claim 1] ... the feature of the original source *including device* configuration status of the original source ... including *an indication of a type of* software *installed on the original resource*”... (emphasis added)

A feature “*including an indication of type of software installed on the original resource”* is different in scope, and more precise, than “*a feature of an original resource* *related to … a software type*."

Applicant's present claim amendments thus are different in scope than the claim language presented on 9/1/2010, and said changes in scope have necessitated further consideration of the prior art, as well as the newly presented grounds of rejection.

***4.*** On page 15, Applicant argues that the presented claims 1, 38, 43, 44 and 50:

> "now include elements admittedly absent from Pazi and Mackay. Thus [said claims] are not rendered obvious over Pazi and Mackay."

Applicant's arguments are not persuasive. As explained above, the newly presented claim language has not been previously presented, and has necessitated reconsideration of the present newly presented combination of Pazi in view of Mackay.

***5.*** Continuing on pages 15 - 16, Applicant argues that nothing in Nilsen:

> "shows or in any way implies a feature related to a configuration status being selected from a group consisting of an operating system type, an operating system version, a software type... The sum total of the allegedly relevant portions of the Nilsen disclosure are set forth below…".

It appears, based on the excerpt provided by Applicant on page 16, that Applicant has interpreted Nilsen as solely showing 5 lines of relevant text. As page 20 of the 8/11/2011 Non-Final rejection noted, however, the rejection was made in view of *pages 1 – 2* of the document titled "how do I detect PROXY?", also referred to as "Nilsen" and not merely the 5 lines of text recited by Applicant on page 16. One of ordinary skill in the art, at the time of the invention, would have interpreted the "Nilsen" disclosure as follows:

Pages 1 – 2 of "how do I detect PROXY?", from alt.comp.lang.php, hereafter Nilsen,

begins with a user “sang” requesting information on how to detect [and ban] user's utilizing proxies. The user "Morten Nilsen" replies that contrary to the opinion of a previously user, “XDude”, proxies can be detected. The example “Morten Nilsen" provides is that "SQUID", a well-known HTTP proxy, indicates when it is in use via a value set in a message header, the header containing "SQUID/[version number of SQUID]”.
The Examiner thus does not agree that it is reasonably to distill the 2 pages of the "Nilsen" reference into the 5 lines addressed by Applicant. Regardless, in view of the clarification provided by the presented claim amendments, a new grounds of rejection has been made as noted below.

***6.*** Applicant’s remaining arguments, relying on the reasoning addressed above, thus are unpersuasive for the reasons given above.

### *Claim Rejections - 35 USC § 103*

***7.*** The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

***8.*** Claims 1- 5, 9 – 23, 32, 34, 38, 43, 44 and 46 – 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi (US 2003/0110274 A1) in view of Mackay (comp.os.ms-windows.networking.tcp-ip. "Can my ISP say if i'm using a proxy?" 2/16/2002. pgs. 1 - 4.).

***9.*** Regarding claim 1, Pazi shows a method of making a determination, the method comprising:

receiving a communication from the potential device, the communication comprising a first information element (*e.g., a claimed source address, [7,15,30]*) and a second information element (*e.g., a TTL from the intercepted communication, [7,15,30]*) wherein the potential device is an original source of said second information element;

identifying a feature of an original source of the first information element (*identifying the "authenticated", "reference" TTL value from the packet, [30,47]*)

identifying a feature of the potential device (*identifying the TTL value in the currently received/incoming packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*)

determining, using a detection system implemented at least in part in hardware, that the feature of the original source of said first information element and the feature of the potential device are features unlikely to relate to a single device (*showing determining when communications are from a bogus/hacker device versus when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]*),

said determining being indicative that the potential device is a device (*showing determining that a packets source is not what is claimed in an received packet and thus a potential bogus/hacker device is such a device; Figs. 2,3, [7-17, 30]*),

Pazi does show a feature of original source and feature of the potential device, but Pazi does not show: the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source,

the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device; and

where the determination is whether the potential device is a relay device and where said detection system is a relay detection system.

Mackay shows: the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source (*pg. 2, describing the "default source port range of says [sic] a windows PC"*),

the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device (*pg. 2, describing checking received packets for particular use of "source port range", "choice of source ports" and "headers such as x-forwarded-for" that are added by application level gateways such as 'wingate' proxy software, to detect the presence and use of "proxy gateways"*); and

making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing "source port range", "headers such as x-forwarded-for" added by application level gateways such as 'wingate' proxy software, and "choice of source ports" of received packets to detect the presence of "proxy gateways"*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

***10.*** Regarding claim 2, Pazi in view of Mackay further show wherein said second information element is of a type that a relay device of a class of relay devices is unlikely to relay (*Mackay, pg. 2*).

***11.*** Regarding claim 3, Pazi in view of Mackay further show wherein said class of relay devices is selected from the group consisting of a SOCKS proxy, an HTTP proxy using the GET method, an HTTP proxy using the CONNECT method, an IP router and a NAT device (*Mackay, pg. 2*).

***12.*** Regarding claim 4, Pazi in view of Mackay further show wherein said second information element is part of a communication, wherein the communication is of a type selected from the group consisting of IP, TCP, ICMP, DNS, HTTP, SMTP, TLS, and SSL (*Mackay, pg. 2*).

***13.*** Regarding claim 5, Pazi in view of Mackay further show wherein said first information element is part of a communication, wherein the communication is of a type selected from the group consisting of IP, TCP, ICMP, DNS, HTTP, SMTP, TLS, and SSL (*Mackay, pg. 2*).

***14.*** Regarding claim 9, Pazi in view of Mackay further show wherein said stage of determining further comprises:

comparing said feature of an original source of said first information element with said feature of the potential relay device (*Pazi, [55]*).

***15.*** Regarding claim 10, Pazi in view of Mackay further show obtaining a parameter indicative of said feature of an original source of said first information element; and

obtaining a parameter indicative of said feature of the potential relay device (*Pazi, [7-17] and Figs. 2, 3*).

***16.*** Regarding claim 11, Pazi in view of Mackay further show wherein said stage of determining further comprises:

considering a time at which at least one of said feature of an original source of said first information element and said feature of the potential relay device, was discovered (*Pazi, [44]*).

***17.*** Regarding claim 12, Pazi in view of Mackay further show obtaining a parameter indicative of a relationship between said feature of said original source of said first information element and said feature of the potential relay device (*Pazi, [44, 50-52]*).

***18.*** Regarding claim 13, Pazi in view of Mackay further show wherein said stage of determining includes analyzing said parameter indicative of a relationship between said feature of said original source of said first information element and said feature of the potential relay device (*Pazi, [44, 50-52]*).

***19.*** Regarding claim 14, Pazi in view of Mackay further show wherein said parameter is obtained from at least one of said first information element and said second information element (*Pazi, [44, 50-52]*).

***20.*** Regarding claim 15, Pazi in view of Mackay further show c) sending an outgoing communication to at least one of said original source of said first information element and the potential relay device (*Pazi, [16]*); and receiving a third information element from said at least one of said original source of said first information element and the potential relay device (*Pazi, [16-18]*).

***21.*** Regarding claim 16, Pazi in view of Mackay further show e) deriving from said third information element information related to a feature of said at least one of said original source of said first information element and the potential relay device (*Pazi, [16-18, 44, 49-52]*).

***22.*** Regarding claim 17, Pazi in view of Mackay further show verifying that an original source of said third information element is said original source of said first information element (*Pazi, [16-18, 47]*).

***23.*** Regarding claim 18, Pazi in view of Mackay further show verifying that an original source of said third information element is the potential relay device (*Pazi, [54]*).

***24.*** Regarding claim 19, Pazi in view of Mackay further show wherein said third information element is selected from the group consisting of an ICMP message, an ICMP Echo Reply message, a DNS query, an HTTP request, an HTTP response, an HTTP `Server` header, an IP address, a TCP port, a TCP Initial Sequence number, a TCP Initial Window, a WHOIS record, and a reverse DNS record (*Mackay, pg. 2 and Pazi, [60-62]*).

***25.*** Regarding claim 20, Pazi in view of Mackay further show wherein at least one of said feature of an original source of said first information element and said feature of the potential relay device is a feature related to a device configuration status including an indication of a type of hardware of the original source or the potential relay device

(*Mackay, pg. 2 discussing a "windows PC" as a original source as well as "gateway devices", "NAT routers" as a potential relay device*).

***26.*** Regarding claim 21, Pazi in view of Mackay further show wherein said feature related to a device configuration status is selected from the group consisting of an operating system type (*Mackay, pg. 2, discussing the Windows OS*), an operating system version a software type, an HTTP client type, an HTTP server type (*Mackay, pg. 2, discussing the application level gateway 'wingate' as an HTTP proxy gateway*), an SMTP client type, an SMTP server type, a time setting, a clock setting and a time zone setting.

***27.*** Regarding claim 22, Pazi in view of Mackay further show wherein said determining includes examining a parameter indicative of said feature related to a device configuration status (*Mackay, pg. 2 discussing devices configured "incorrectly" or configured to utilize specific ranges of source ports and/or specific proxy software*).

***28.*** Regarding claim 23, Pazi in view of Mackay further show wherein said parameter is selected from the group consisting of an HTTP 'User-Agent' header, an RFC 822 'X-Mailer' header, an RFC 822 'Received' header, an RFC 822 'Date' header, a protocol implantation manner (*Mackay, pg. 2, discussing incorrect implementation of ICMP, as well as particular implementations of HTTP*), a TCP/IP stack fingerprint, an IP address, a TCP port (*Mackay, pg. 2*), a TCP initial sequence number, a TCP initial window a WHOIS record, and a reverse DNS record.

***29.*** Regarding claim 32, Pazi in view of Mackay further show wherein at least one of said feature of an original source of said first information element and said feature of the potential relay device is selected from the group consisting of a sub-network (*Pazi, [47,52]*), an administrator, and a location (*Mackay, pgs. 1 – 2 and Pazi, [35]*).

***30.*** reverse DNS record (*Mackay, pg. 2*)

***31.*** Regarding claim 34, Pazi shows a method of determining whether a potential device is a device, the method comprising:

receiving from the potential device a first information element (*e.g., a claimed source address, [7,15,30]*) and a second information element (*e.g., a claimed source address, [7,15,30]*) wherein the potential device is an original source of said second information element

analyzing a configuration status of an original source of at least one of said first and said second information elements (*Pazi, [7-17]*)

identifying a feature of an original source of the first information element (*identifying the "authenticated", "reference" TTL value from the packet, [30,47]*)

identifying a feature of the potential device (*identifying the TTL value in the currently received/incoming packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*)

determining, using a detection system, whether the feature of an original source of said first information element and the feature of the potential device are features unlikely to relate to a single device (*showing determining when communications are from a bogus/hacker device versus when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]*).

Pazi does not show: said configuration status selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting, and a time zone setting;

the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source,

the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device; and

where the determination is whether the potential device is a relay device and where said detection system is a relay detection system.

Mackay shows: said configuration status selected from the group consisting of an operating system type (*Mackay, pg. 2, discussing the Windows OS*), an operating system version, a software type, an HTTP client type, an HTTP server type (*Mackay, pg. 2, discussing the application level gateway 'wingate' as an HTTP proxy gateway*), an SMTP client type, an SMTP server type, a time setting, a clock setting, and a time zone setting;

the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source (*pg. 2, describing the "default source port range of says [sic] a windows PC"*),

the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device (*pg. 2, describing checking received packets for particular use of "source port range", "choice of source ports" and "headers such as x-forwarded-for" that are added by application level gateways such as 'wingate' proxy software, to detect the presence and use of "proxy gateways"*); and

making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing TTL values of received packets to detect the presence of devices*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

***32.*** Regarding claim 38, Pazi shows a method of making a determination, the method comprising:

receiving from the potential device a first information element (*e.g., a claimed source address, Pazi [7,15,30]*) and a second information element (*e.g., a TTL value, Pazi [7,15,30]*);

identifying a feature of an original source of the first information element (*identifying the "authenticated", "reference" TTL value from the first information element packet, [30,47]*);

identifying a feature of an original source of the second information element (*identifying the TTL value in the currently received/incoming second information element* *packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*);

determining, using a detection system that the feature of an original source of said first information element and the feature of the original source of said second information element are features unlikely to relate to a single device (*showing determining when communications are from a bogus/hacker device versus when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]*),

said determining being indicative that the potential device is a device (*showing determining that a packets source is not what is claimed in an received packet and thus a potential bogus/hacker device is such a device; Figs. 2,3, [7-17, 30]*),

Pazi does show a feature of original source and feature of the potential device, but Pazi does not show: the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source,

the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device; and

where the determination is whether the potential device is a relay device and where said detection system is a relay detection system.

Mackay shows: the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source (*pg. 2, describing the "default source port range of says* *[sic] a windows PC"*),

the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device (*pg. 2, describing checking received packets for particular use of "source port range", "choice of source ports" and "headers such as x-forwarded-for" that are added by application level gateways such as 'wingate' proxy software, to detect the presence and use of "proxy gateways"*); and

making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing "source port range", "headers such as x-forwarded-for" added by application level gateways such as 'wingate' proxy software, and "choice of source ports" of received packets to detect the presence of "proxy gateways"*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

***33.*** Regarding claim 43, Pazi shows a method of determining whether a potential device is a device, the method comprising:

identifying a feature of an original source of a first information element (*e.g., a claimed source address, [7,15,30]*);

identifying a feature of the potential device that transmitted the first information element and a second information element, the potential device being the original source of the second information element (*e.g., identifying a "authenticated", "reference" TTL value from the packet, [30,47], as well as identifying a TTL from the intercepted communication, [7,15,30]*); and

determining, using a detection system, whether a feature of an original source of a first information element and a feature of the potential device are features unlikely to relate to a single device (*showing determining when communications are from a bogus/hacker device versus when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]*),

wherein a positive result of said determining is indicative that the potential device is a device (*showing determining that a packets source is not what is claimed in an received packet and thus a potential bogus/hacker device is such a device; Figs. 2,3, [7-17, 30]*).

Pazi does show a feature of original source and feature of the potential device, but Pazi does not show: the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source,

the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device; and

where the determination is whether the potential device is a relay device and where said detection system is a relay detection system.

Mackay shows: the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source (*pg. 2, describing the "default source port range of says [sic] a windows PC"*),

the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device (*pg. 2, describing checking received packets for particular use of "source port range", "choice of source ports" and "headers such as x-forwarded-for" that are added by application level gateways such as 'wingate' proxy software, to detect the presence and use of "proxy gateways"*); and

making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing "source port range", "headers such as x-forwarded-for" added by application level gateways such as 'wingate' proxy software, and "choice of source ports" of received packets to detect the presence of "proxy gateways"*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

***34.*** Regarding claim 44, Pazi shows a system, implemented at least in part in hardware, to determine whether a potential device is a device, the system comprising:

a processor (*Fig. 1*);

a feature database (*Fig. 2, items 42 and 52, [47]*) in data communication with the processor,

an information element receiver, executable by the processor, to receive information elements from a plurality of devices including an information source device and the potential device (*[7,15,30]*);

a feature discovery module, executable by the processor, to identify at least one of a feature of the information source device (*e.g., identifying the "authenticated", "reference" TTL value from the packet, [30,47]*) and a feature of the potential device (*e.g., identifying the TTL value in the currently received/incoming packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*);

a feature incompatibility analyzer, executable by the processor and in data communication with the a feature database (Pazi, [9,30]), to determine whether the feature of said information source device and the feature of the potential device are features unlikely to relate to a single device (*showing determining when communications are from a bogus/hacker device versus when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]*).

Pazi does show a feature of original source and feature of the potential device, but Pazi does not show: the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source,

the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device; and

where the determination is whether the potential device is a relay device and where said detection system is a relay detection system.

Mackay shows: the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source (*pg. 2, describing the "default source port range of says [sic] a windows PC"*),

the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device (*pg. 2, describing checking received packets for particular use of "source port range", "choice of source ports" and "headers such as x-forwarded-for" that are added by application level gateways such as 'wingate' proxy software, to detect the presence and use of "proxy gateways"*); and

making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing "source port range", "headers such as x-forwarded-for" added by application level gateways such as 'wingate' proxy software, and "choice of source ports" of received packets to detect the presence of "proxy gateways"*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

***35.*** Regarding claim 46, Pazi in view of Mackay further show wherein the information element receiver is further configured to receive information elements from a monitored host (*Pazi, [55-58,61]*).

***36.*** Regarding claim 47, Pazi in view of Mackay further show an outgoing information element sender executable by the processor (*Pazi, [61]*).

***37.*** Regarding claim 48, Pazi in view of Mackay further show a parameter obtainer, executable by the processor, for obtaining at least one parameter selected from the group consisting of a parameter indicative of a feature of an information source device, a parameter indicative of a feature of the potential relay device, and a parameter indicative of whether a feature of said information source device and a feature of said potential relay device are features unlikely to relate to a single device (*Pazi, Figs. 2 and 3, [52]*).

***38.*** Regarding claim 49, Pazi in view of Mackay further show where the feature database for storing a map between pairs of features and data indicative of whether said pairs of features are incompatible features (*Pazi, [47,54]*).

***39.*** Regarding claim 50, Pazi shows a computer-readable non-transitory storage medium, comprising instructions, which when executed by a computer cause the computer to:

receive from the potential device a first information element (*e.g., a claimed source address, [7,15,30]*) and a second information element (*e.g., a claimed source address, [7,15,30]*) wherein the potential device is an original source of said second information element;

identifying a feature of an original source of the first information element (*identifying the "authenticated", "reference" TTL value from the packet, [30,47]*)

identifying a feature of the potential device (*identifying the TTL value in the currently received/incoming packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*)

determine whether the feature of an original source of said first information element and the feature of the potential device are features unlikely to relate to a single device (*showing determining when communications are from a bogus/hacker device versus when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]*),

wherein a positive result of said determining is indicative that the potential device is a device (*showing determining that a packets source is not what is claimed in an received packet and thus a potential bogus/hacker device is such a device; Figs. 2,3, [7-17, 30]*).

Pazi does show a feature of original source and feature of the potential device, but Pazi does not show: the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source,

the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device; and

where the determination is whether the potential device is a relay device and where said detection system is a relay detection system.

Mackay shows: the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source (*pg. 2, describing the "default source port range of says [sic] a windows PC"*),

the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device (*pg. 2, describing checking received packets for particular use of "source port range", "choice of source ports" and "headers such as x-forwarded-for" that are added by application level gateways such as 'wingate' proxy software, to detect the presence and use of "proxy gateways"*); and

making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing "source port range", "headers such as x-forwarded-for" added by application level gateways such as 'wingate' proxy software, and "choice of source ports" of received packets to detect the presence of "proxy gateways"*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

***40.*** Claims 7 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay as applied to claim 1 above, and further in view of Reed (Applying the OSI Seven Layer Network Model to Information Security. November 21, 2003).

***41.*** Regarding claim 7, Pazi in view of Mackay show claim 1.

Pazi in view of Mackay do not show wherein said first and said second information elements are sent in two different layers of a protocol stack.

Reed shows wherein said first and said second information elements are sent in two different layers of a protocol stack (*Reed, pg. 24*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Reed in order to exploit common knowledge relating to networking and information security (Reed, pg. 1).

***42.*** Regarding claim 33, Pazi in view of Mackay show claim 32.

Pazi in view of Mackay do not show wherein said determining includes examining a parameter indicative of at least one of said feature of a source of said first communication and said feature of a source of said second communication, and said parameter is selected from the group consisting of an HTTP `User-Agent` header, an RFC 822 `X-Mailer` header, an RFC 822 `Received` header, an RFC 822 `Date` Header, an IP address, a WHOIS record, and a reverse DNS record.

Reed shows wherein said determining includes examining a parameter indicative of at least one of said feature of a source of said first communication and said feature of a source of said second communication, and said parameter is selected from the group consisting of an HTTP `User-Agent` header, an RFC 822 `X-Mailer` header, an RFC 822 `Received` header, an RFC 822 `Date` Header, an IP address, a WHOIS record, and a reverse DNS record (*Reed, pgs. 23 – 24*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Reed in order to exploit common knowledge relating to networking and information security (Reed, pg. 1).

***43.*** Claims 24 – 31, 35 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay as applied to claim 1 above, and further in view of Daude (US 6,892,235 B1).

***44.*** Regarding claim 24, Pazi in view of Mackay show claim 1.

Pazi in view of Mackay do not explicitly show wherein at least one of said feature of a source of said first information element and said feature of the potential relay device is a feature related to communication performance.

Daude shows wherein at least one of said feature of a source of said first information element and said feature of the potential relay device is a feature related to communication performance (*col. 7 lines 25 - 34, Figs. 5 – 7*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Daude in order to use automatic methods to analyze and better understand the network (*Daude, col. 7 lines 25 - 34*)

***45.*** Regarding claim 25, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is selected from the group consisting of a measured communication performance, a measured relative communication performance, and an estimated communication performance (Daude, Figs. 5 – 7).

***46.*** Regarding claim 26, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is selected from the group consisting of a latency of communication, a latency of an incoming communication, a latency of an outgoing communication, a round trip time of a communication, a communication rate, an incoming communication rate, an outgoing communication rate, a maximum communication rate, an incoming maximum communication rate, and an outgoing maximum communication rate (Daude, col. 8 lines 36 – 40).

***47.*** Regarding claim 27, Pazi in view of Mackay and Daude further show wherein said determining includes examining a parameter indicative of said feature related to communication performance (*Pazi, [34]*).

***48.*** Regarding claim 28, Pazi in view of Mackay and Daude further show wherein said parameter is selected from the group consisting of time of receipt of an information element, time of sending of an information element, a round trip time, a round trip time gap, an IP address, a Whois record, a reverse DNS record, and a rate of acknowledged information (*Daude, col. 8 lines 36 – 40*).

***49.*** Regarding claim 29, Pazi in view of Mackay and Daude further show wherein a higher round trip time gap is indicative of a higher likelihood that a relay device is being used for malicious purposes (*Daude, col. 8 lines 60 – 65*).

***50.*** Regarding claim 30, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is estimated from information about at least one of said original source of said first communication and the potential relay device (Daude, Abstract).

***51.*** Regarding claim 31, Pazi in view of Mackay and Daude further show wherein said information about at least one of said original source of said first communication and the potential relay device is selected from the group consisting of a location of a device, a reverse DNS record of a device's IP address, and an administrator of a device (*Daude, col. 11 lines 48 – 60*).

***52.*** Regarding claim 35, Pazi shows a method of determining whether a potential device is a device, the method comprising:

receiving from the potential device a first information element (*e.g., a claimed source address, [7,15,30]*) and a second information element (*e.g., a claimed source address, [7,15,30]*) wherein the potential device is an original source of said second information element;

analyzing, using a detection system, a feature of an original source of at least one of said first and said second information elements (*e.g., identifying the "authenticated", "reference" TTL value from the packet, [30,47]*);

identifying a feature of an original source of the first information element (*identifying the "authenticated", "reference" TTL value from the packet, [30,47]*);

identifying a feature of the potential device (*identifying the TTL value in the currently received/incoming packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*);

determining, using a detection system, whether a feature of an original source of said first information element and a feature of the potential device are features unlikely to relate to a single device (*showing determining when communications are from a bogus/hacker device versus when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]*),

Pazi does show a feature of original source and feature of the potential device, but Pazi does not show: the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source,

the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device; and

where the determination is whether the potential device is a relay device and where said detection system is a relay detection system.

Mackay shows: the feature including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source (*pg. 2, describing the "default source port range of says [sic] a windows PC"*), the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device (*pg. 2, describing checking received packets for particular use of "source port range", "choice of source ports" and "headers such as x-forwarded-for" that are added by application level gateways such as 'wingate' proxy software, to detect the presence and use of "proxy gateways"*); and

making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing "source port range", "headers such as x-forwarded-for" added by application level gateways such as 'wingate' proxy software, and "choice of source ports" of received packets to detect the presence of "proxy gateways"*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

Pazi in view of Mackay do not show where the identified features include communication performance, and analyzing a feature related to communication performance of an original source of at least one of said first and said second information elements.

Daude shows where identified features include communication performance, and analyzing a feature related to communication performance of an original source of at least one of said first and said second information elements (*col. 7 lines 25 – 34, Figs. 5*

*– 7*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Daude in order to use automatic methods to analyze and better understand the network (*Daude, col. 7 lines 25 – 34*).

***53.*** Regarding claim 36, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is selected from the group consisting of a latency of communication, a latency of an incoming communication, a latency of an outgoing communication, a round trip time of a communication, a communication rate, an incoming communication rate, an outgoing communication rate, a maximum communication rate, an incoming maximum communication rate, and an outgoing maximum communication rate (*Daude, col. 8 lines 36 – 40*).

## *Conclusion*

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M. MacIlwinen whose telephone number is (571) 272-9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glen Burgess, can be reached on (571) 272 - 3949. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JOHN MACILWINEN/

Primary Examiner, Art Unit 2442

(571) 272 - 9686